



MAT-8067US

PATENT #4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Y. Murakawa

: Art Unit: 2131

Serial No.: 09/729,262

: Examiner:

Filed: December 1, 2000

: Box Missing Parts

FOR: METHOD OF VIRTUAL PRIVATE

:

NETWORK COMMUNICATION IN

:

SECURITY GATEWAY APPARATUS AND

SECURITY GATEWAY APPARATUS

USING THE SAME

CLAIM TO RIGHT OF PRIORITY

Assistant Commissioner for Patents

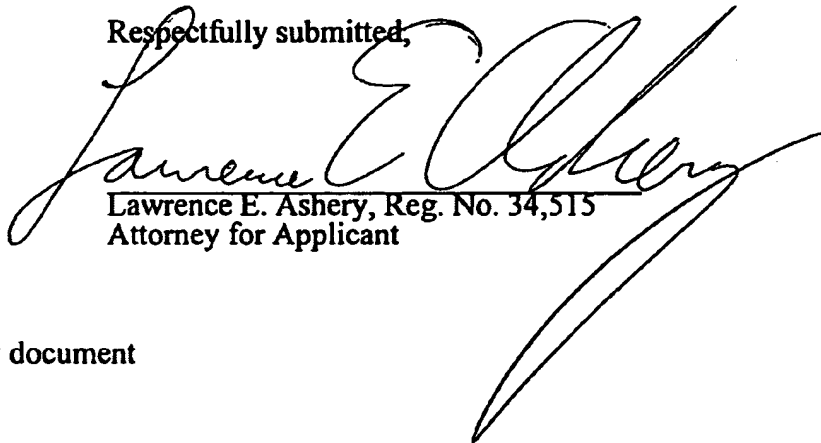
Washington, D.C. 20231

S I R :

Pursuant to 35 U.S.C. 119, Applicant's claim to the benefit of filing of prior Japanese Patent Application No. 11-344500, filed December 3, 1999, is hereby confirmed.

A certified copy of the above-referenced application is enclosed.

Respectfully submitted,



Lawrence E. Ashery, Reg. No. 34,515
Attorney for Applicant

LEA/dlm

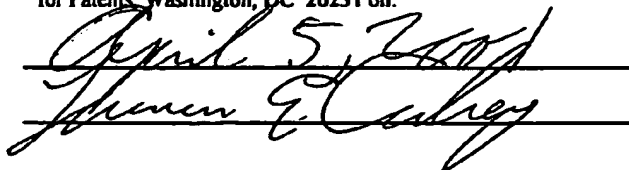
Encl.: (1) certified priority document

Dated: April 5, 2001

Suite 301, One Westlakes, Berwyn
P.O. Box 980
Valley Forge, PA 19482
(610) 407-0700

The Assistant Commissioner for Patents is hereby authorized to charge payment to Deposit Account No. 18-0350 of any fees associated with this communication.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231 on:

April 5, 2001




original, doc.
MAT-8067US

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年12月 3日

出願番号

Application Number:

平成11年特許願第344500号

出願人

Applicant(s):

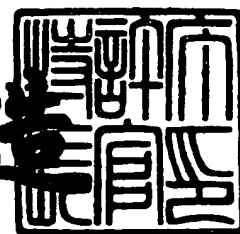
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年11月10日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3094181

【書類名】 特許願

【整理番号】 2913011174

【提出日】 平成11年12月 3日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/28

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 村川 泰

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100097445

 【弁理士】

 【氏名又は名称】 岩橋 文雄

【選任した代理人】

 【識別番号】 100103355

 【弁理士】

 【氏名又は名称】 坂口 智康

【選任した代理人】

 【識別番号】 100109667

 【弁理士】

 【氏名又は名称】 内藤 浩樹

【手数料の表示】

 【予納台帳番号】 011305

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 セキュリティ・ゲートウェイ装置におけるVPN通信方法

【特許請求の範囲】

【請求項1】 公衆回線などから構成されるWANとLANとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるVPN通信方法であって、ダイヤルアップ接続でWANに接続した外部のPCに対してIPsecプロトコルによりVPNを実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリングされたIPパケットにおけるIPsec処理される送信元IPアドレスの指定を実現するセキュリティ・ゲートウェイ装置におけるVPN通信方法。

【請求項2】 IKE通信時に、セキュリティ・ゲートウェイ装置配下のLANと同じセグメントのIPアドレス/サブネットマスクアドレスをダイヤルアップ接続からLANにアクセスする前記外部のPCに割り当て、前記外部のPCを仮想的にLAN環境下に置いたVPN通信を実現する請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法。

【請求項3】 NAT技術を組み合わせて前記外部のPCにLAN配下で使用しているプライベートIPアドレスをIKE通信時に付与し、プライベートIPアドレスで構築されたLAN環境への前記外部のPCからのアクセスが可能なVPN通信を実現するセキュリティ・ゲートウェイ装置におけるVPN通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数のPCを接続したLANと公衆回線などのWAN（Wide Area Network）とを集線・変換処理を行うことにより接続するセキュリティ・ゲートウェイ装置で構成されるネットワーク環境において、公衆回線にダイヤルアップ接続した外部のPCがWANを介してセキュリティ・ゲートウェイ装置とVPN（Virtual Private Network、仮想専用網）通信を行うためのセキュリティ・ゲートウェイ装置におけるVPN通信方法に関するものである。

【0002】

【従来の技術】

近年、企業のみならず家庭に至るまで複数台のPCが導入され、インターネットへの接続が進んでいる。複数台のPCで構成されるLANをインターネットに接続する場合、LANとWANを接続するゲートウェイ装置が必要になる。また、LANの外部のPCからLAN配下の端末にアクセスするには、まず契約しているプロバイダにダイヤルアップ接続し、WAN経由でLAN配下の端末（例えばPC）にアクセスすることになる。

【0003】

しかし、WANを流れるパケットは基本的に安全性が確保されておらず、パケットを盗聴されると、第三者に通信内容を悪用される恐れがある。通信内容の秘匿性と外部からの不正アクセスを防止するためには、WANとLANを接続するセキュリティ・ゲートウェイ装置が必要となり、ダイヤルアップ接続するPCにもセキュリティのための通信プロトコルスタックが実装されてないといけない。そして、外部からアクセスするPC（外部のPC）とセキュリティ・ゲートウェイ装置の間でVPN通信を行うことで、WAN上で仮想的な専用線環境が実現できる。現在、VPN通信のための代表的な通信プロトコルとして実装されているのはIPsec (Security Architecture for the Internet Protocol) である。

【0004】

以下に、IPsecを利用したVPN通信の概要を説明する。まず図4を参照しながら説明する。図4はWANを含む一般的なネットワークシステムを示す構成図である。

【0005】

図4において、101はプロバイダにダイヤルアップ接続した外部のPC、102はWAN、103はWAN102と後述のLAN104を接続して集線・変換処理を行うセキュリティ・ゲートウェイ、104はセキュリティ・ゲートウェイ103配下のLAN、105はLAN104上のサーバ端末、106、107はLAN104上のクライアントPC、108はPC101とセキュリティ・ゲ

ートウェイ 103 との間で IPsec 通信を行うために確立された VPN である。

【0006】

ダイヤルアップ接続した PC101 が LAN104 上の端末にアクセスする場合、セキュリティ・ゲートウェイ 103 との間で VPN108 を確立し、WAN102 上で仮想的な専用線環境を実現する。こうして WAN102 上で通信内容を盗聴・改竄できないようにし、LAN104 配下の端末と通信を行う。

【0007】

次に、IPsec 通信を行うために必要な通信内容の概要について図 5 を用いて解説する。図 5 は WAN による接続を示す WAN 接続図である。

【0008】

図 5 において、PC101、WAN102、セキュリティ・ゲートウェイ 103 は図 4 と同様のものである。

【0009】

PC101 とセキュリティ・ゲートウェイ 103 との 2 点間で IPsec 通信を行う場合、データの秘匿性、コネクションレスな完全性（相手との論理的な通信路を構築せず、データの改ざんを防止すること）、改ざん防止などを保証するための暗号アルゴリズム、認証アルゴリズムに用いる鍵情報を両者が IPsec 通信を行う前に共有できてないといけない。両者で鍵情報を共有させる方法として、事前に両者で鍵情報を手動で設定する方法と、IKE (Internet Key Exchange) プロトコルを用いて自動設定する方法の 2 通りがある。ここでは、現実的な方法である IKE プロトコルによる自動鍵情報交換方式のみを適用する。

【0010】

次に、図 6 を用いて IPsec 通信について説明する。図 6 は IPsec 通信開始のためのセキュリティ・ゲートウェイ 103 の動作を示すフローチャートである。

【0011】

IPsec 通信を行うためには、2 点間で双方向に論理的なコネクション SA

(Security Association) を確立しなければならない。そのためにIKE通信は2つのフェーズに分かれていて、フェーズ1において安全なIKE通信を行うためのIKE-SAを確立しようとし(S11、S12)、それに成功したら、フェーズ2において、IPsec通信するための鍵情報などのセキュリティ情報を交換する(S13)。フェーズ2でIPsec-SAを確立することができれば(S14)IKE通信を終了し、IPsec通信が開始する(S15)。ステップS13のIKE(フェーズ2)通信においてIPsec通信を行うために2点間で交換される情報を(表1)に示す。

【0012】

【表1】

項 目	詳 細
セキュリティ・プロトコル	ESP/AH
IPsec通信モード	トンネルモード/トランスポートモード
暗号アルゴリズム	ESPの場合必須
暗号鍵	—
認証アルゴリズム	AHの場合必須、ESPでも選択可
認証鍵	—
SAの寿命形式	データ量(バイト)/時間(量)
SAの寿命	—

【0013】

但し動作モード(IPsec通信モード)については、セキュリティ・ゲートウェイ103はトンネルモード(IPパケット全体をカプセリングする)でしか動作できないので、ここでは、IPsecの動作モードはトンネルモードのみを想定する。

【0014】

図7はトンネルモードのIPsec通信の概要を示す説明図である。

【0015】

図7において、PC101、セキュリティ・ゲートウェイ103、LAN104、クライアントPC106、VPN108は図4と同様のものである。100はIPパケットである。

【0016】

図7において、PC101、セキュリティ・ゲートウェイ103、クライアントPC106のIPアドレスをそれぞれA、B、Cとする（AはプロバイダによってPC101に付与されたIPアドレス）。LAN104上のクライアントPC106からVPN108を介してコネクションの張られたPC101にIPパケットを送信する場合、まずクライアントPC106において、送信元IPアドレスがC、宛先IPアドレスがAのIPパケット100が作成され、送信される。セキュリティ・ゲートウェイ103がこのパケット100を受信し、VPN108を張られたPC101宛てのパケットであることを識別すると、IKE通信による交換した情報に基づいてIPパケット100をカプセリングする。元のIPアドレスの外側に、送信元IPアドレスB、宛先IPアドレスAのIPヘッダが付加される。このとき交換した情報に基づいてカプセリングされたIPパケットへの認証情報の付加、暗号化が行われる。VPN108を介してカプセリングされたパケットを受信したPC101は、交換した情報に基づいてカプセリングされた元のIPパケット100を取り出し、処理する。

【0017】

【発明が解決しようとする課題】

しかしながら、上記従来のセキュリティ・ゲートウェイ装置におけるVPN通信方法では、WAN102上でのデータの安全性は確保できているが、あくまで外部ネットワークからのアクセスと判断されるため、LAN104配下のクライアントPC106の情報にアクセスするために、LAN104配下のクライアントPC106に設定（アクセス許可／不許可を示すセキュリティ・ポリシーの設定、例えば許可するIPアドレスと不許可となるプロトコル・サービスなど）が必要になり、その設定のために別の安全性の問題が生じる可能性があり、LAN104がプライベートIPアドレスで構成されたネットワークの場合、その設定

は特に困難になるという問題点を有していた。

【0018】

このセキュリティ・ゲートウェイ装置におけるVPN通信方法では、WANを介して外部からアクセスするPCを仮想的にLAN配下の端末として通信可能にすることが要求されている。

【0019】

本発明は、この要求を満たすため、WANを介して外部からアクセスするPCを仮想的にLAN配下の端末として通信可能にするセキュリティ・ゲートウェイ装置におけるVPN通信方法を提供することを目的とする。

【0020】

【課題を解決するための手段】

この課題を解決するために本発明のセキュリティ・ゲートウェイ装置におけるVPN通信方法は、公衆回線などから構成されるWANとLANとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるVPN通信方法であって、ダイヤルアップ接続でWANに接続した外部のPCに対してIPsecプロトコルによりVPNを実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリングされたIPパケットにおけるIPsec処理される送信元IPアドレスの指定を実現する構成を備えている。

【0021】

これにより、WANを介して外部からアクセスするPCを仮想的にLAN配下の端末として通信可能にするセキュリティ・ゲートウェイ装置におけるVPN通信方法が得られる。

【0022】

【発明の実施の形態】

本発明の請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法は、公衆回線などから構成されるWANとLANとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるVPN通信方法であって、ダイヤルアップ接続でWANに接続した外部のPCに対してIPsecプロ

トコルによりVPNを実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリングされたIPパケットにおけるIPsec処理される送信元IPアドレスの指定を実現することとしたものである。

【0023】

この構成により、セキュリティ・ゲートウェイ装置は、ダイヤルアップ接続した外部のPCとIPsec通信する際、そのPCの最終的な宛先IPアドレスを制御可能にし、LAN配下の端末への設定を不要とし、安全性が確保されるという作用を有する。

【0024】

請求項2に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法は、請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法において、IKE通信時に、セキュリティ・ゲートウェイ装置配下のLANと同じセグメントのIPアドレス／サブネットマスクアドレスをダイヤルアップ接続からLANにアクセスする外部のPCに割り当て、外部のPCを仮想的にLAN環境下に置いたVPN通信を実現することとしたものである。

【0025】

この構成により、VPNを確立した外部のPCがLAN環境内にあるように仮想的にみなせる作用を有する。

【0026】

請求項3に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法は、請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法において、NAT技術を組み合わせて外部のPCにLAN配下で使用しているプライベートIPアドレスをIKE通信時に付与し、プライベートIPアドレスで構築されたLAN環境への外部のPCからのアクセスが可能なVPN通信を実現することとしたものである。

【0027】

この構成により、プライベートIPアドレスで構成されたLAN環境に、安全性を確保したまま外部のPCからのアクセスを可能にするという作用を有する。

【0028】

以下、本発明の実施の形態について、図1～図3を用いて説明する。

【0029】

(実施の形態1)

図3は、本発明の実施の形態1によるセキュリティ・ゲートウェイ装置におけるVPN通信方法において用いるIKE通信データフォーマットを示すフォーマット図である。

【0030】

図3に示す通り、IKE通信はUDP (User Datagram Protocol) / IP (Internet Protocol) を使用して行われる。IKEデータは、ISAKMP (Internet Security Association and Key Management Protocol) ヘッダの後にISAKMPペイロードが数珠つなぎの形態で続くことで構成される。IKE通信は、鍵交換を要求する始動者 (イニシエータ、Initiator) とそれに対して応答する応答者 (リスポンダ、Responder) によって行われる。本実施の形態においては、図4において、プロバイダにダイヤルアップしてインターネットに接続したPC101がInitiatorとなり、LAN104上の端末としてのクライアントPC106、107にアクセスするために、セキュリティ・ゲートウェイ103にIKE通信を開始し、セキュリティ・ゲートウェイ103がResponderとしてIKE通信を行う。(表1) に挙げた項目のうち、暗号鍵と認証鍵は、公開鍵暗号方式を用いてInitiatorとResponderの間で鍵情報が交換されるが、それ以外の項目は、Initiatorが提案をし、ResponderがInitiatorの提案の中から最適なものを選択して応答するというサーバ/クライアントモデルで行われる。DHCP (Dynamic Host Configuration Protocol) クライアントとしてのPC101が取得すべき必須の情報として、IPアドレス、サブネットマスク、IPアドレスの有効期限、ドメイン名がある。これら4つの情報をIKE通信においてResponderであるセキュリティ・ゲートウェイ103が通常のIKEデータでオブショ

ンとして付加する。但し、IPアドレスの有効期限はIKE通信によって確立されるSAの寿命と同じと考えることで省略することができる。またDHCPもUDPの上位に位置するアプリケーションプロトコルなので、IKEに組み込んで再送制御その他の問題は起こらない。

【0031】

図1は本発明の実施の形態1におけるIPsec通信の概略を示す説明図である。

【0032】

図1において、PC101、セキュリティ・ゲートウェイ103、LAN104、クライアントPC106、VPN108は図4と同様のものである。

【0033】

図1において、PC101、セキュリティ・ゲートウェイ103、クライアントPC106のIPアドレスをそれぞれA、B、Cとする（AはプロバイダによってPC101に付与されたIPアドレス）。また、IPsec通信に先立つIKE通信により、セキュリティ・ゲートウェイ103は、PC101にIPアドレスDを配布する。LAN104上のクライアントPC106からVPN108を介して接続の張られたPC101にIPパケットを送信する場合、まずクライアントPC106において、LAN104外部でプロバイダによってPC101に割り当てられたIPアドレスAを意識することなく、送信元IPアドレスがC、宛先IPアドレスがDのIPパケット109が作成され、送信される。セキュリティ・ゲートウェイ103がこのパケット109を受信し、VPN108を張られたPC101宛てのパケットであることを識別すると、IKE通信による交換した情報に基づいてIPパケット109をカプセリングする。元のIPアドレスの外側に、送信元IPアドレスB、宛先IPアドレスAのIPヘッダが付加される。このとき交換した情報に基づいてカプセリングされたIPパケットへの認証情報の付加、暗号化が行われる。VPN108を介してカプセリングされたパケットを受信したPC101は、交換した情報に基づいてカプセリングされた元のIPパケット109を取り出し、IKE通信により取得したサブネットマスク、ドメイン名を元にIPパケット109を処理する。

【0034】

図2はセキュリティ・ゲートウェイ103がPC101にIPアドレスDを配布する手順を示すフローチャートである。

【0035】

IPsec通信を行うためには、2点間で双方向に論理的なコネクションSAを確立しなければならない。そのためにIKE通信は2つのフェーズに分かれていて、フェーズ1において安全なIKE通信を行うためのIKE-SAを確立しようとし(S1、S2)、それに成功したら、フェーズ2において、IPsec通信するための鍵情報などのセキュリティ情報を交換する(S3)。フェーズ2でIPアドレスDを配布し、IPsec-SAを確立することができれば(S4)IKE通信を終了する(S5)。ステップS3のIKE(フェーズ2)通信においてIPsec通信を行うために2点間で交換される情報は(表1)に示す通りである。

【0036】

以上のように本実施の形態によれば、ダイヤルアップ接続でWAN102に接続したPC101に対してIPsecプロトコルによりVPN108を実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリングされたIPパケットにおけるIPsec処理される送信元IPアドレスの指定(アドレスCの指定)を実現するようにしたことにより、セキュリティ・ゲートウェイ103は、ダイヤルアップ接続した外部のPC101とIPsec通信する際、そのPCの最終的な宛先IPアドレスAを制御可能にし、LAN104配下のクライアント端末106への設定を不要とすることができるので、通信内容の盗聴、改竄のおそれが無くなり、安全性を確保することができる。

【0037】

(実施の形態2)

本発明の実施の形態2によるセキュリティ・ゲートウェイ装置におけるVPN通信方法を図1を用いて説明する。

【0038】

図1において、IKE通信のResponderであるセキュリティ・ゲートウェイ103からInitiatorであるPC101にDHCP情報を配布する際に、セキュリティ・ゲートウェイ103配下のLAN104と同じセグメントのIPアドレス、サブネットマスクを配布する。VPN108確立後のIPsec通信において、VPN108上を流れるパケット以外は、LAN104外部から接続するPC101も、セキュリティ・ゲートウェイ103配下のクライアント端末106とネットワークセグメント上区別のない、しかも一意な端末として通信を行う。

【0039】

以上のように本実施の形態によれば、IKE通信時に、セキュリティ・ゲートウェイ103配下のLAN104と同じセグメントのIPアドレス／サブネットマスクアドレスをダイヤルアップ接続からLAN104にアクセスするPC101に割り当て、外部のPC101を仮想的にLAN104環境下に置いたVPN通信を実現するようにしたことにより、VPN108を確立した外部のPC101がLAN104環境内にあるように仮想的にみなすことができるので、安全性を確保したまま外部からLAN104内の端末にアクセスすることができる。

【0040】

(実施の形態3)

本発明の実施の形態3によるセキュリティ・ゲートウェイ装置におけるVPN通信方法を図1を用いて説明する。

【0041】

図1において、セキュリティ・ゲートウェイ103がNAT (Network Address Translator) 技術を用い、セキュリティ・ゲートウェイ103配下のLAN104をプライベートIPアドレスのみで構成していた場合、通常は外部からLAN104上のクライアント端末106にはアクセスできないが、ダイヤルアップ接続したPC101とセキュリティ・ゲートウェイ103がVPN108を確立するためのIKE通信の中で、セキュリティ・ゲートウェイ103配下のLAN104で使用されているセグメントにおける、まだ使用されていないプライベートIPアドレスをIKEに組み込んだDHCP

オプションにより PC101 に配布することにより、WAN102 上にある VPN108 上はグローバル IP アドレスで通信しながら、LAN104 内、そして PC101 の内部では、プライベート IP アドレスでネットワークセグメント上区別のない、しかも一意な端末として通信を行うことができる。

【0042】

以上のように本実施の形態によれば、NAT 技術を組み合わせて外部の PC101 に LAN104 配下で使用しているプライベート IP アドレスを IKE 通信時に付与し、プライベート IP アドレスで構築された LAN104 環境への外部からのアクセスが可能な VPN 通信を実現するようにしたことにより、プライベート IP アドレスで構成された LAN104 環境に、安全性を確保したまま外部の PC101 からのアクセスが可能になる。

【0043】

【発明の効果】

以上説明したように本発明の請求項 1 に記載のセキュリティ・ゲートウェイ装置における VPN 通信方法によれば、公衆回線などから構成される WAN と LAN との間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置における VPN 通信方法であって、ダイヤルアップ接続で WAN に接続した外部の PC に対して IPsec プロトコルにより VPN を実現する際、IPsec 通信に先立つ IKE 通信時に、DHCP 通信オプションを IKE データに統合し、トンネリングされた IP パケットにおける IPsec 処理される送信元 IP アドレスの指定を実現することにより、セキュリティ・ゲートウェイ装置は、ダイヤルアップ接続した外部の PC と IPsec 通信する際、その PC の最終的な宛先 IP アドレスを制御可能にし、LAN 配下の端末への設定を不要とすることができるので、安全性を確保することができるという有利な効果が得られる。

【0044】

請求項 2 に記載のセキュリティ・ゲートウェイ装置における VPN 通信方法によれば、請求項 1 に記載のセキュリティ・ゲートウェイ装置における VPN 通信方法において、IKE 通信時に、セキュリティ・ゲートウェイ装置配下の LAN と同じセグメントの IP アドレス／サブネットマスクアドレスをダイヤルアップ

接続から LAN にアクセスする外部の PC に割り当て、外部の PC を仮想的に LAN 環境下に置いた VPN 通信を実現することにより、VPN を確立した外部の PC が LAN 環境内にあるように仮想的にみなすことができるので、安全性を確保したまま外部から LAN 内の端末にアクセスすることができるという有利な効果が得られる。

【 0 0 4 5 】

請求項 3 に記載のセキュリティ・ゲートウェイ装置における VPN 通信方法によれば、請求項 1 に記載のセキュリティ・ゲートウェイ装置における VPN 通信方法において、NAT 技術を組み合わせて外部の PC に LAN 配下で使用しているプライベート IP アドレスを IKE 通信時に付与し、プライベート IP アドレスで構築された LAN 環境への外部の PC からのアクセスが可能な VPN 通信を実現することにより、プライベート IP アドレスで構成された LAN 環境に、安全性を確保したまま外部の PC からのアクセスが可能になるという有利な効果が得られる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 における IPsec 通信の概略を示す説明図

【図 2】

セキュリティ・ゲートウェイが外部の PC に IP アドレスを配布する手順を示すフローチャート

【図 3】

本発明の実施の形態 1 によるセキュリティ・ゲートウェイ装置における VPN 通信方法において用いる IKE 通信データフォーマットを示すフォーマット図

【図 4】

WAN を含む一般的なネットワークシステムを示す構成図

【図 5】

WAN による接続を示す WAN 接続図

【図 6】

IPsec 通信開始のためのセキュリティ・ゲートウェイ装置の動作を示すフ

ローチャート

【図 7】

トンネルモードの IPsec 通信の概要を示す説明図

【符号の説明】

101 PC

102 WAN

103 セキュリティ・ゲートウェイ

104 LAN

105 サーバ端末

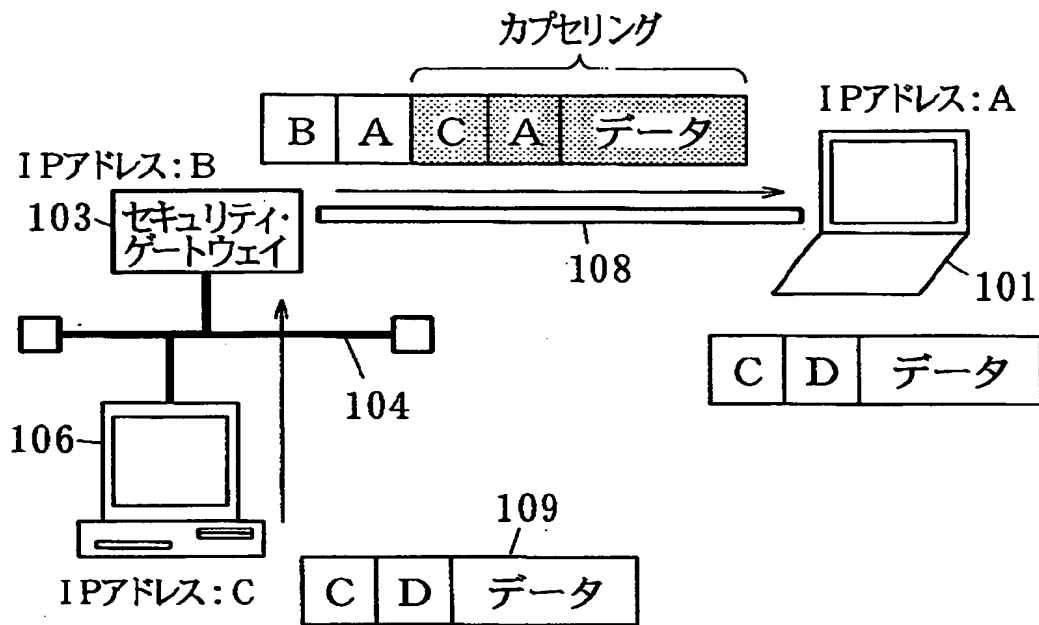
106、107 クライアント端末（クライアント PC）

108 VPN

109 IP パケット

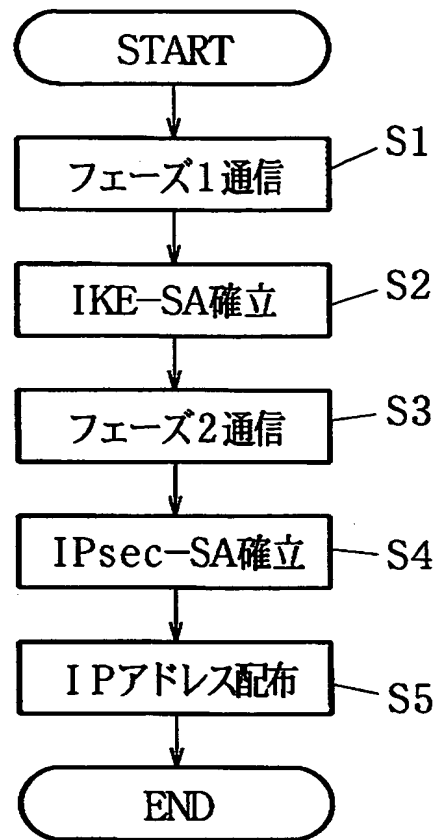
【書類名】 図面

【図 1】

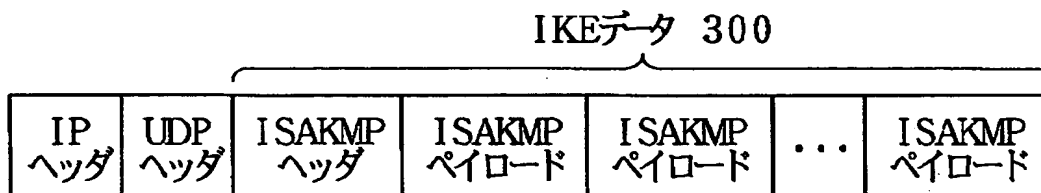


- 101 PC
- 103 セキュリティ・ゲートウェイ装置
- 104 LAN
- 106 クライアント端末(クライアントPC)
- 108 VPN
- 109 IPパケット

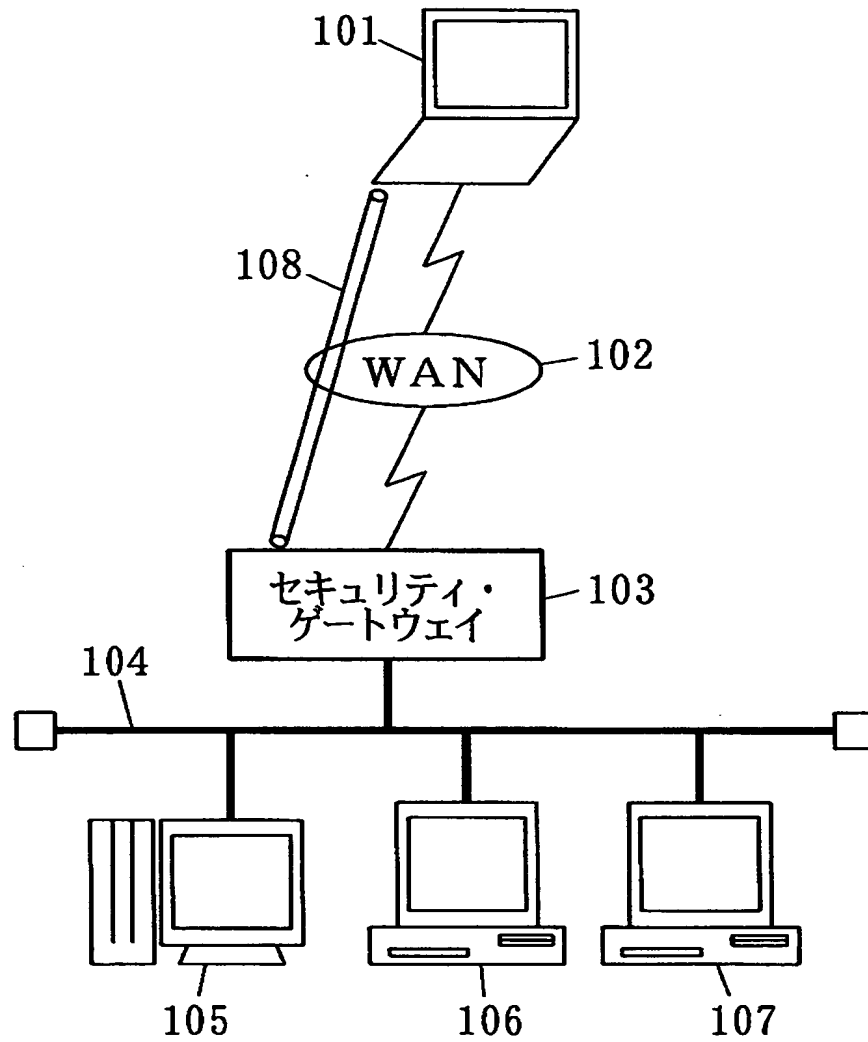
【図 2】



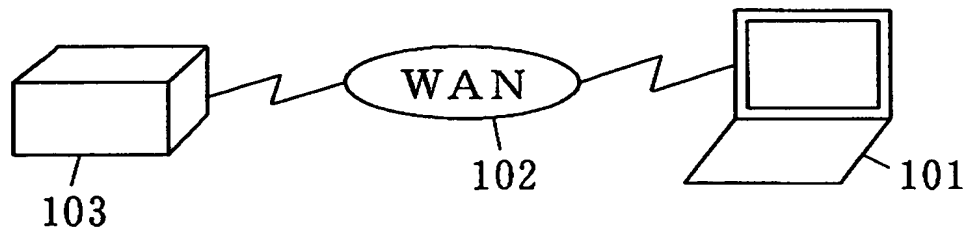
【図 3】



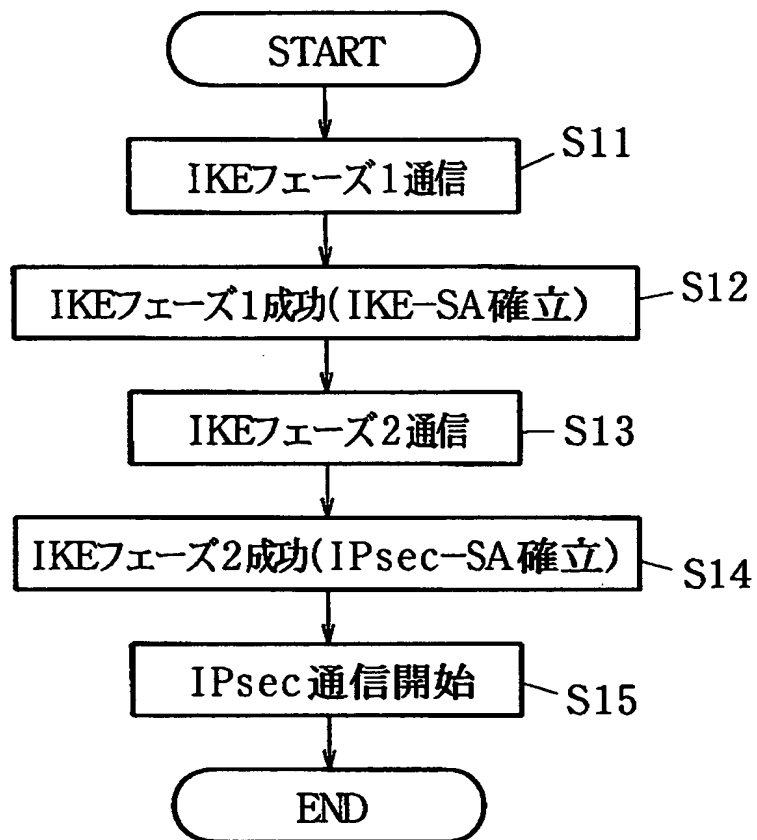
【図4】



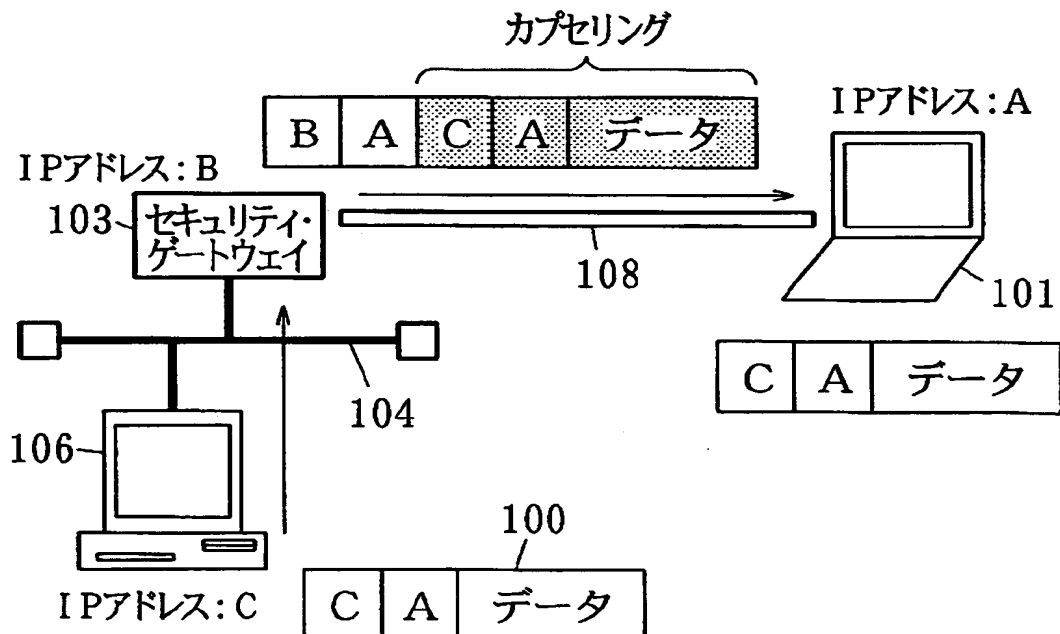
【図5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 W A N を介して外部からアクセスする P C を仮想的に L A N 配下の端末として通信可能にするセキュリティ・ゲートウェイ装置における V P N 通信方法を提供することを目的とする。

【解決手段】 公衆回線などから構成される W A N と L A N 104 との間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置 103 における V P N 通信方法であって、ダイヤルアップ接続で W A N に接続した外部の P C 101 に対して I P s e c プロトコルにより V P N 108 を実現する際、 I P s e c 通信に先立つ I K E 通信時に、 D H C P 通信オプションを I K E データに統合し、トンネリングされた I P パケットにおける I P s e c 処理される送信元 I P アドレス C の指定を実現する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社